International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 2, Apr 2015, 1-6
TJPRC Pvt. Ltd.

SECCLOUD USING MULTI-DIMENSIONAL ACCESS: A SURVEY

AHIRE RAHUL, TEMPE BHUSHAN KUMAR, KELGANE GIRISH & GAURIBHAGAT

K.J's Educational Institute's, Trinity College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT

Cloud computing is latest style of computing where everything from computing world utilizes in an infrastructure, and various business application are provided then provided "as a services ".Cloud computing is not a newly developed technology it is just a way of reusing old services in effective manner.

Data leakage is one of the sensitive problems in many of the established organizationsacross the world .There are a number of security issues associated with cloud computing which can be broadly categories as security issues faced by cloud providers and security issues faced by their cloud users. Hence the responsibility goes in both ways.The provider must ensure about their infrastructure is secure and that their client'sdata and applications are protected on the other side the user must take care to secure their applications and use strong passwords and authentication measures to achieve it. Hence Security is quit challenging and difficult when cloud computing is concerned. Some of the securities issues are like insider threat attacks difficulty in physical access control etc.in order to provide reliable cloud service's existing technique resolve these issues partially.

Hence our focus is to study security related issues and their solutions if exist and will try to build robust system to access cloud services by enhancing existing techniques.

KEYWORDS: Cloud Computing, Data Leakage, Authentication, Robust System, Cloud Services

INTRODUCTION

Cloud computing is rapid growing technology which provides on-demand software, hardware, infrastructure and data storage as services. This technology is used worldwide to improve the business infrastructure and performance. For accessing the data stored on cloud it is necessary to have stronger password authentication. Now a day's cloud password authentication can be done in several ways like textual password, image based password. Prerequisites for design cloud computing data security model are cloud computing technology architecture and its features. Cloud computing service provider delivers. The applications via internet. Web browsers are the connecting media between user and the cloud. Cloud Computing services are classified into 3 sections which are (SaaS) Software as a Service, (IaaS) Infrastructure as a Service and (PaaS) Platform as a Service. SaaS provides different software's as a services via internet regardless of its installation over the user's computers. Host user gets the platform through the Paas for its application IaaS deliver's virtualized environment nothing but the computer infrastructure for the user application.

By considering security aspect of cloud computing our dream is to build a robust system to store the user's confidential data. Our approach will be like; we try to provide multi-level security access to the cloud data. At the first level, simple textual password authentication will provide to the user. This type of authentications generally used for less confidential data to be stored. Hence we will keep it at first level. In the second level we will use encryption and decryption

technique along with OTP (one time password) to enhance the security level. Lastly, the technique called Graphical user based authentication will be used to achieve high level of security. Because in this type of authentication it is difficult to crack graphical password by untrusted user as compare to the normal textual password.

LITERATURE SERVEY

As we focusing on the Security of Cloud for the purpose of secure data storage, it will be better to have study of existing techniques. So we have performed literature survey of some previous papers, basis on which we are trying to build our system more effective.

Parikshit Prasad et.al, have proposed a system to focus on the data leakage problem and designed a framework to securely access data over cloud in [1].Cloud computing is newly arrived technology in the market, so along with its advantages it also having new issues and challenges to protect data. Cloud computing is based on virtualizationconcept where services like Saas,Paas and Iaasare provided and their introduction is provided in this paper. They defined a basics of cloud storage and its security where they mentioned problem that though the cloud computing is emerging technology most of the companies not using cloud to store data because of Data leakage issue. The framework they designed was divided intotwo phases. In the first phase, user need to be provide the data which want to be upload over the cloud along with its value of security in terms of (C) Confidentiality, (I) Integrity and (A) Availability. In the second phase, cloud server provides the secure access to the users data based on the level of security that user needed.The security was provided by server in three levelwhere at first level less confidential data managed by providing user ID and password. In second level password provided on user's mail account and at a third level high level of security achieved by sending One Time Password(OTP) on user's mobile.Though the three level securities provided in this paper,some drawbacks we noticed like need of hardware and hence system implementation cost increased.

Shraddha M. Guravet. al., have proposed their work using Graphical password authentication process [2] paper. As the enhancement in the authentication process, the graphical password is one of the best and simple alternative method for alphanumeric or text password. Strong authentication system possible to design using graphical password. Because graphical password contains images such as photos, artificial pictures or other kind of images. Before implementation authors of this paper performed related study in which they mentioned some relative methods by considering their advantages and disadvantages. For ease of understanding, they made comparison among these methods contains six categories of schemes which are Image based, Grid based, Traingle based, Hybrid textual, Signature based and Username-image password scheme. After performing survey they stated that applications are more secure with graphical password. Because it is easy to remember the graphical password as compared to alphanumeric password by user. They performed experimental evaluation to get access to the cloud data.In this paper,two options were provided to the client that are Sign in and Sign up. During the Sign up process provided by server side, User need to be enter the appropriate username. Using the algorithm server provided image set. Initially, username verification is done. After that set of images are provided touser among which user must select two images and then server select two images for that particular user.By combining these two selection pattern complete password getting stored in server database. Now, valid user can perform sign in to the system. In sign in process, the user have to give their valid username which they had given at the time of sign up process and then they need to be select the password fromgiven set of images for the purpose of authentication. Validation of user is done then cloudaccess is given to particular user. They access their accountwith uploading and downloading facility.Graphical password in the means of image based that will be photo,artificial picture,or

other kind of image .It will be difficult for hacker to guess the graphical password than textual password. Beside this advantage, in case of multiple accounts of same person, this image based authentication system may be less active because in that case it will be difficult to memorize multiple graphical passwords each of which contains unique series of images.

In this paper [3], Housam KhalifaBashier et. al., were proposed system based on The EdgePass algorithm. They start their work in this paper with small introduction that, In general, there are two approaches in graphical password authentication scheme stated as:

- Recall Based
- Recognition based.

In Recall Based password user must select to generate an event or to reproduce it at the time of registration. But, the main problem with this approach is that it depends heavily on precise recall of secret information. Whereas in case of recognition based password two subtypes are like decoy and pass image are used.The decoy images are randomly generated by the system during the verification process and pass-images are users selected images.

Then they researched on some other methods to enforce their system. In that they studied hash visualization algorithm in which random images were generated by system called random art. For access to the data, valid user was required torecognize the pass-images from a challenge image set. In the next scheme, monochrome was generated from the user pass-images so that the it looked noisy. But, disadvantage found in this was it hard for valid users to recognize the pass-images because the images were noisy and blur to users that was resulted into time consuming authentication. They also studied method where low frequency component of the decoy images were combined with high frequency component of the pass-images by user.

To overcome the problems due to previous methods, Edge detection which algorithm wasbased on detection of physical properties as well as geometrical properties of an objects.They also introduced a new algorithm used in this paper to calculate area in a plane bounded by a graph.During Edge pass, estimation was taken in account that whether the process pixel wasdark or light. If it waslight then the target pixel was considered to be anedge, else it was abackground. Advantage of this system they thought was like; if the number of images in the challenge set wereappropriately large then there was provision of higher password space than the normal textualpassword. We think that, most of the solutions defined in this paper are complex, time consuming and lack of usability.

In the paper [4], SunitaBhatiet. al. they designed an algorithm in the world of cryptography. Cryptography is an art of secretly transmitting our messages to the intended recipients. To achieve this, the original text or plaintext, is translated into anencrypted formor we can say in the cipher text, which is then sent to thevalid user. Then that user decrypts the received message into its original form. After performing survey the authors of this paper conclude that whichever previous algorithms were there to securely transfer of message had some drawbacks. Though the algorithms like AES, DES were used in strongly secured system. Along with the improvement in the speed, the complexity and time also get increased. To solve this problem, authors of this paper proposed (BREA)Byte Rotation Encryption Algorithm. They decided to design it because its following features:

- It is Public Key Block Cipher Algorithm.
- Block size is of 16 bytes.

- Key matrix is of size 16 bytes.
- Randomly selected key matrix values that are ranging from 1 to 26.
- Byte-Rotation scheme is used.

Sonia Chiassonet. al. proposed a graphical password authentication system based on (PCCP)Persuasive cued click-points technique in [5]. As there was problem regarding text-based password.Users create recognizable passwords that were easyfor attackers to guess, but strong system-assignedpasswords were difficult for users as well to remember. Hence, by adding a PCCP features to the authentication system encourages users to select less predictable passwords and makes it difficult for invalid users or hackers to select passwords where all five click-points are hotspots. During the password creation, the selected images by user getting slightly shaded except for a viewport. Then selection by users must be as a click-point within that highlighted viewport and it is restricted outside the viewport area, unless they click on the shuffle button to randomly change the position of the viewport.

By studying all related papers we have decided to design a system that will be the improvement to some extent for few existing techniques. So we have tried to design multilevel secure model which includes three authentication rings that are ring 1, ring 2 and ring 3 respectively.This is client-server in which, user is at client side and cloud act as server. At client side, firstly user going to provide C,I,A values for his data to be stored on cloud server, then at server side these values are evaluated and helps to categories requested data, to its appropriate security level. After deciding the security level for particular file, our system will provide different policies based on protection levels. These levels are ring 1, ring 2 and ring 3. Ring 1 will be at outer layer; ring 3 will be at innermost layer and ring 2 will be in between ring 1 and ring 3.Less confidential data should be in ring1 without any authentication rules to be applied. Ring 2 contains a data whose security need is lie between ring 1 and ring 3 that means this data need limited security. The data with highest security must be in ring 3.In this way our system works to provide reliable access to the user's data.

CONCLUSIONS

Our proposed system will overcome the problems due to insider threat attacks, data leakage in an organizations etc. The main achievement for our system will be strong and multilevel authentication for user's data that to be stored on cloud, because by knowing the simple textual password user may get access to the outer layer but will not be able to enter in next layer so access to the confidential data on cloud will be more difficult for untrusted users.

In future, try to design a system by using different approach and algorithms that will give us comparatively less time complexity and more user friendly system.

ACKNOWLEDGEMENTS

We would like to thanks our project guide Prof. GauriBhagatand Head of the Department Prof. BilkisChandargi for giving us their valuable guidance and for providing all the necessary facilities which were helpful in the completion of this project review. We would like to express our gratitude towards all the other faculty members of I.T Department for their valuable time, support, comments, and suggestions.

REFERENCES

1. Parikshit Prasad, BadrinathOjha, Rajeev RanjanShahi, RatanLal,AbhishekVaishAndUtkarshGoel, "3 Dimensional Security In Cloud Computing", IEEE [2011].
2. Shraddha M. Gurav, Leena S. Gawade, Prathamey K. RaneAndNilesh R. Khochare, "Graphical Password Authentication", International Conference On Electronic Systems, Signal Processing And Computing Technologies [2014].
3. HousamKhalifaBashier, Lau SiongHoeAnd Pang Ying Han, "Graphical Password: Pass-Images Edge Detection", IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac. 2013, Kuala Lumpur, Malaysia [2013].
4. SunitaBhati, Anita Bhati and S. K. Sharma, "A New Approach Towards Encryption Schemes: Byte – Rotation Encryption Algorithm", Proceedings Of The World Congress On Engineering And Computer Science, Vol I Wcecs, [2012].
5. Sonia Chiasson, ElizabethStobert, Alain Forget, Robert Biddle and Paul C. Van Oorschot, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, March/April [2012].
6. Fawaz A Alsulaiman and abdulmotaleb El Saddik, "A Novel 3d Graphical Password Schema", IEEE International Conference on Virtual Environments, Human-Computer Interfaces, And Measurement Systems July [2006].
7. G.Ganeshsriram, B, SM. K P Gupta, Vijayaaditya and R. Santosh Kumar, "Application Study on Cloud Computing Based Virtual Campus Paper", IJIET, Vol. 2 Issue 1 February [2013].
8. Rafael A. Calvo, Stephen T. O'rourke, Janet Jones, KalinaYacef and Peter Reimann, "Collaborative Writing Support Tools on the Cloud", IEEE Transactions on Learning Technologies, Vol. 4, No. 1, January-March [2011].
9. Vrushali Joshi, PayalSanghvai and Yogita Bhargude, "Three Tier Data Storage Securityin Cloud Using Face Fuzzy Vault", International Journal Of Internet Computing ISSN No: 2231 – 6965, Vol- 1, Iss- 3 [2012].
10. FarnazTowhidi and Maslin Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms", International Journal of Computer Science and Information Security, Vol. 6, No. 2 [2009].
11. Ting Wang, Yu Xia, Zhiyang Su, And Mounir Hamdi, "Rethinking The Data Center Networking", IEEE Access, Volume 2 [2012].
12. Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks In The Cloud", IEEE Symposium On Security And Privacy Workshops [2012].
13. Wei Xie, Lei Xie, Chen Zhang, Quan Zhang and Chaojing Tang, IEEE International Conference On RFID[2013].
14. Meng Cheng, Ray Y. Zhong,Yuanyuan Li, HaoLuo, ShulinLan And George Q. Huang, "Cloud Service-Oriented Dashboard For Work Cell Management In RFID-Enabled Ubiquitous Manufacturing", IEEE [2013].
15. Maninder Singh AndSarbjeet Singh, "Design and Implementation of Multi-Tier Authentication Scheme In Cloud", IJCSI International Journal Of Computer Science Issues, Vol. 9, Issue 5, No 2, September [2012].

16. Cong Wang, Bingsheng Zhang, KuiRen, And Janet M. Roveda, "Privacy-Assured Outsourcing Of Image Reconstruction Service In Cloud", IEEE Transactions On Emerging Topics, Volume 1, No. 1, June [2013].
17. Mohammed A.Alzain, Eric Pardede, Ben Soh And James A. Thom,"Cloud Computing Security: From Single To Multi-Clouds", IEEE 45th Hawaii International Conference On System Sciences [2012].
18. Florian Pfarr, Thomas Buckel and Axel Winkelmann, "Cloud Computing Data Protection – A Literature Review And Analysis", IEEE 47th Hawaii International Conference On System Science[2014].